DETAILED ACTION

1. The Examiner contacted the applicant's undersigned attorney, Brian L. Klock to include dependent claim to base claims to independent claims to particulary pointout the invention and clarify 101 problem and fix typo. Brian L. Clock authorized the examiner to amend the claims by examiner's amendment as shown below.

Response to Amendment

2. The IDS submitted on 8/6/09 is considered except the Europe search report. English translation of the Europe search report is required.

Response to Arguments

3. Applicants arguments submitted on 09/15/2009 are fully considered and are persuasive.

EXAMINER'S AMENDMENT

4. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Applicant's representative, Brian L. Klock on October 7, 2009.

Claims:

Claims **1, 6, 7, 13, 16, and 19** are amended and claims **3 and 9** are cancelled.

1. (Currently Amended) An authentication apparatus having a plurality of authentication mechanisms, characterized by comprising:

an input unit adapted to input authentication information of an object of authentication, said authentication information having been already authenticated by a first mechanism that is in use;

a determination unit adapted to determine whether the authentication information that has been input by said input unit corresponds to an object of authentication that has an authority to change over the first authentication mechanism in use to another authentication mechanism;

a display control unit adapted to display a list of the plurality of authentication mechanisms if it has been determined by said determination unit that the authentication information that has been input corresponds to the object of authentication that has the authority to make the changeover;

a registration unit adapted to register, as an effective authentication mechanism, a second authentication mechanism that has been selected from the list displayed by said display control unit;

a verification unit adapted to verify that authentication of the object of authentication in the second authentication mechanism succeeds; and

a changeover control unit adapted to control management of the object of authentication so that successful authentication of the object of authentication in the second authentication

mechanism is verified before management is changed over from the first authentication mechanism to the second authentication mechanism,

wherein the first authentication mechanism and the second authentication mechanism are managed by a common start-up unit,

wherein changeover of management of the object of authentication, which has been successfully authenticated in the first authentication mechanism, from the first authentication mechanism to the second authentication mechanism is initiated in response to selection of the second authentication mechanism as an effective authentication mechanism, [and]

wherein the object of authentication continues to be in an authenticated state in the first authentication mechanism, and is not released from management under the first authentication mechanism, until successful authentication in the second authentication mechanism is verified,

wherein said input unit reads a card on which authentication information of an object of authentication has been recorded and inputs said authentication information, and

wherein the changeover control unit is a central processing unit.

3. (Cancelled)

6. (Currently Amended) The authentication apparatus according to claim [[1]] 1, further having a start-up unit for starting up an authentication mechanism that has been registered as an effective authentication mechanism by said registration unit.

7. (Currently Amended) An authentication method of changing over a plurality of authentication mechanisms and performing authentication with anyone of said plurality of authentication mechanisms, comprising:

an input step of inputting authentication information of an object of authentication, said authentication information having been already authenticated by a first authentication mechanism that is in use;

a determination step of determining whether the authentication information that has been input at said input step corresponds to an object of authentication that has an authority to change over the first authentication mechanism in use to another authentication mechanism;

a display control step of displaying a list of the plurality of authentication mechanisms if it has been determined at said determination step that the authentication information that has been input corresponds to the object of authentication that has the authority to make the changeover;

a registration step of registering, as an effective authentication mechanism, a second authentication mechanism that has been selected from the list displayed at said display control step;

a verification step of verifying that authentication of the object of authentication in the second authentication mechanism succeeds; and

a changeover control step of controlling management of the object of authentication so that successful authentication of the object of authentication in the second authentication mechanism is verified before management is changed over from the first authentication mechanism to the second authentication mechanism,

wherein the first authentication mechanism and the second authentication mechanism are managed by a common start-up unit,

wherein changeover of management of the object of authentication, which has been successfully authenticated in the first authentication mechanism, from the first authentication mechanism to the second authentication mechanism is initiated in response to selection of the second authentication mechanism as an effective authentication mechanism, [[and]]

wherein the object of authentication continues to be in an authenticated state in the first authentication mechanism, and is not released from management under the first authentication mechanism, until successful authentication in the second authentication mechanism is verified,

wherein one or more of the foregoing steps is performed using a processor, and

wherein a card on which authentication information of an object of authentication has been recorded is read and said authentication information is input at said input step.

9. (Cancelled)

13. (Currently Amended) An authentication method comprising:

an input step of inputting authentication information of an object of authentication;

a first authentication step of authenticating whether an object of authentication has access right to a first system using the authentication information of the object of authentication that has been input at said input step, and allowing the object of authentication to access the first system if authentication succeeds;

a second authentication step of authenticating whether the object of authentication has access right to a second system using the authentication information of the object of authentication that has been input at said input step, and allowing the object of authentication to access the second system if authentication succeeds;

a control step of controlling whether the object of authentication will be managed under management of the first system or under management of the second system; and

a verification step of verifying that authentication of the object of authentication in the second system has succeeded at said second authentication step;

wherein the first system and the second system are managed by a common start-up unit,

wherein changeover of management of the object of authentication, which has been successfully authenticated in the first system, from the first system to the second system is initiated in response to an instruction to switch the object of authentication from management under the first system to management under the second system,

wherein if an instruction is recognized, that instructs to switch the object of authentication that is authenticated at the first authentication step from management under the first system to management under the second system, said control step performs control so that successful authentication of the object of authentication in the second system is verified before management is changed over from the first system to the second system,

wherein the object of authentication continues to be in an authenticated state in the first system, and is not released from management in the first system, until successful authentication in the second system is verified, [[and]]

wherein one or more of the above steps is performed using a processor,

wherein said input step reads a card on which authentication information of an object of authentication has been recorded and inputs said authentication information.

16. (Currently Amended) An authentication apparatus comprising:

an input unit adapted to input authentication information of an object of authentication;

a first authentication unit adapted to authenticate whether an object of authentication has access right to a first system using the authentication information of the object of authentication that has been input by said input unit, and allowing the object of authentication to access the first system if authentication succeeds;

a second authentication unit adapted to authenticate whether the object of authentication has access right to a second system using the authentication information of the object of authentication that has been input by said input unit, and allowing the object of authentication to access the second system if authentication succeeds;

a control unit adapted to control whether the object of authentication will be managed under management of the first system or under management of the second system; and

a verification unit adapted to verify that authentication of the object of authentication in the second system by said second authentication unit has succeeded;

wherein the first system and the second system are managed by a common start-up unit,

wherein changeover of management of the object of authentication, which has been successfully authenticated in the first system, from the first system to the second system is initiated in response to an instruction to switch the object of authentication from management under the first system to management under the second system,

wherein if an instruction is recognized, that instructs to switch the object of authentication that is authenticated at the first authentication step from management under the first system to management under the second system, said control unit performs control so that successful authentication of the object of authentication in the second system is verified before management is changed over from the first system to the second system, and

wherein the object of authentication continues to be in an authenticated state in the first system, and is not released from management in the first system, until successful authentication in the second system is verified,

wherein said input unit reads a card on which authentication information of an object of authentication has been recorded and inputs said authentication information, and

wherein the control unit is a central processing unit.

19. (Currently Amended) An authentication program stored in a computer-readable storage medium comprising:

code for implementing an input step of inputting authentication information of an object of authentication;

code for implementing a first authentication step of authenticating whether an object of authentication has access right to a first system using the authentication information of the object of authentication that has been input at said input step, and allowing the object of authentication to access the first system if authentication succeeds;

code for implementing a second authentication step of authenticating whether the object of authentication has access right to a second system using the authentication information of the object of authentication that has been input at said input step, and allowing the object of authentication to access the second system if authentication succeeds;

code for implementing a control step of controlling whether the object of authentication will be managed under management of the first system or under management of the second system; and

code for implementing a verification step of verifying that authentication of the object of authentication in the second system has succeeded at said second authentication step;

wherein the first system and the second system are managed by a common start-up unit,

wherein changeover of management of the object of authentication, which has been successfully authenticated in the first system, from the first system to the second system is

initiated in response to an instruction to switch the object of authentication from management under the first system to management under the second system,

wherein if an instruction is recognized, that switches the object of authentication that is authenticated at the first authentication step from management under the first system to management under the second system: said control step performs control so that successful authentication of the object of authentication in the second system is verified before management is changed over from the first system to the second system, and

wherein the object of authentication continues to be in an authenticated state in the first system, and is not released from management in the first system, until successful authentication in the second system is verified,

wherein said input step reads a card on which authentication information of an object of authentication has been recorded and inputs said authentication information.

Allowable Subject Matter

5. Claims **1, 4, 5, 6, 7, and 10-19** are allowed and claims **2, 3, 8 and 9** are canceled.

6. Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Conclusion

7. Any inquiry concerning this communication or earlier communications from the examiner should be directed to ELENI A. SHIFERAW whose telephone number is (571)272-3867. The examiner can normally be reached on Mon-Fri 8:00am-5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser R. Moazzami can be reached on (571) 272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Nasser G Moazzami/

Supervisory Patent Examiner, Art Unit 2436

/Eleni A Shiferaw/

Examiner, Art Unit 2436